

Tor

Internet Anonymity

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!
Brought to you by Abu Ink al Terra

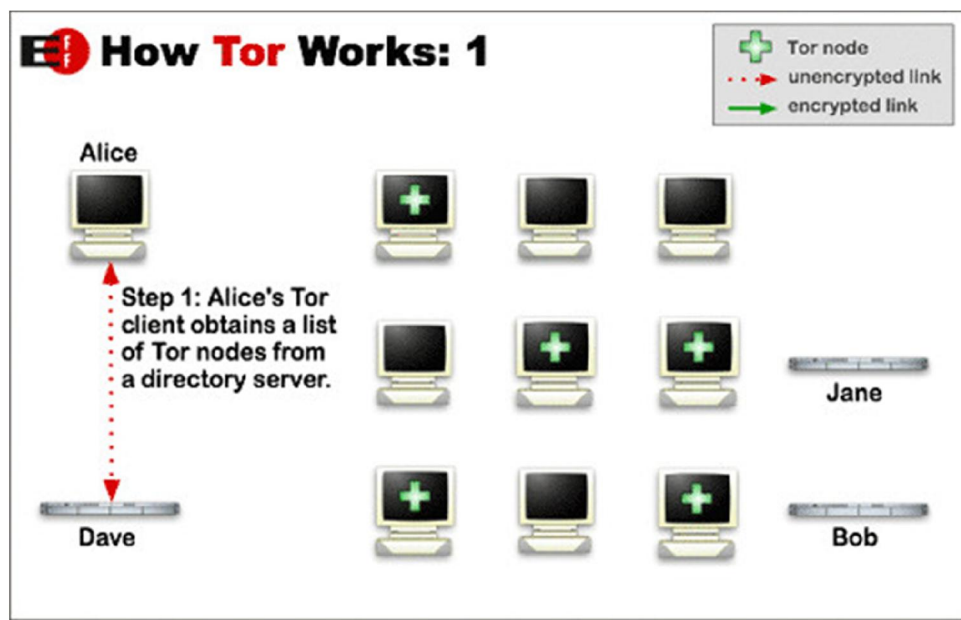
**PLEASE SPREAD THIS TUTORIAL TO INCREASE AWARENESS AMONG MY BELOVED BROTHERS
AND SISTERS ON THE BLESSED PATH!**

What Is Tor Project

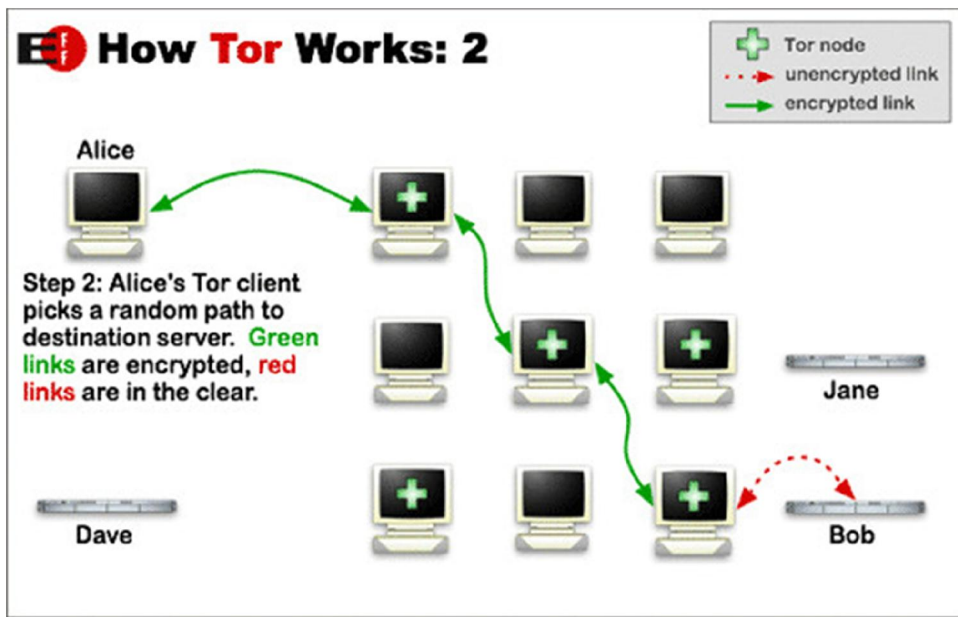
To sum up Tor briefly, imagine driving a car with a different car registration plate every time or whenever you want, if anyone tries to find your car or track it down it makes it very difficult for the pursuer.

HOW TOR WORKS?

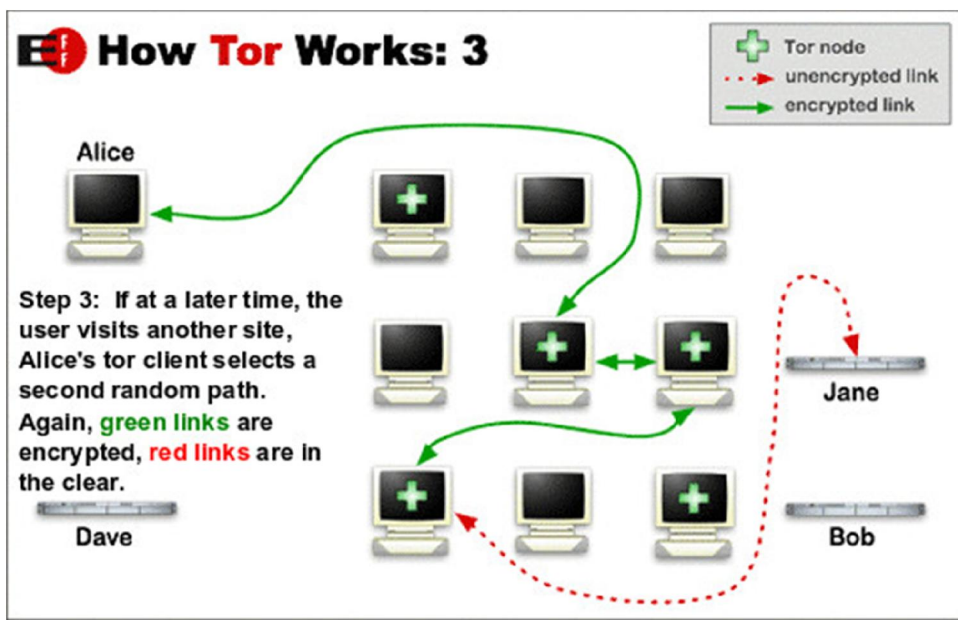
The following three graphics, taken from the Tor Project website itself, explain the process fairly easily.



First, the client's Tor-enabled software determines the list of available Tor nodes that are present in the network. By doing so, it ensures a random node selection each time so that no pattern can be observed by anyone spying, ensuring that you remain private throughout your activities. Random path selection also leaves no footprints, as no Tor node is aware of the origin or destination other than the terminal ones receiving from the clients. And since, from the millions of Tor nodes available, anyone can act as the first receiving node, therefore it is virtually impossible to trace the origin.



Now, the client generates an encrypted message which is relayed to the first Tor node. The Onion router on this node would peel off one layer of encryption and read the information identifying the second node. The second node would repeat the same process and pass on to third. This would go on until the final node receives the location of the actual recipient, where it transmits an unencrypted message to ensure complete anonymity.



Finally, when the client computer wants to establish another path, suppose to visit another website, or even the same one, the Tor network will select an entirely different, random path this time.

[Visit Tor Project Website](#)

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to.

1. Use the Tor Browser

Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor. To avoid problems with Tor configuration, we strongly recommend you use the [Tor Browser Bundle](#). It is pre-configured to protect your privacy and anonymity on the web as long as you're browsing with the Tor Browser itself. Almost any other web browser configuration is likely to be unsafe to use with Tor.

2. Don't enable or install browser plugins

The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into the Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy. The lack of plugins means that Youtube videos are blocked by default, but Youtube does provide an experimental opt-in feature ([enable it here](#)) that works for some videos.

3. Use HTTPS versions of websites

Tor will encrypt your traffic [to and within the Tor network](#), but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, the Tor Browser Bundle includes [HTTPS Everywhere](#) to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a [blue or green URL bar button](#), include [https://](#) in the URL, and display the proper expected name for the website.

4. Don't open documents downloaded through Tor while online

The Tor Browser will warn you before automatically opening documents that are handled by external applications. **DO NOT IGNORE THIS WARNING.** You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer, downloading the free [VirtualBox](#) and using it with a [virtual machine image](#) with networking disabled, or using [Tails](#). Under no circumstances is it safe to use [BitTorrent and Tor](#) together, however.

5. Use bridges and/or find company

Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a [Tor bridge relay](#) rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more [diverse](#) their interests, the less dangerous it will be that you are one of them. Convince other people to use Tor, too!

Be smart and learn more. Understand what Tor does and does not offer. This list of pitfalls isn't complete, and we need your help [identifying and documenting all the issues](#).

TOR Tutorial

In the name of Allah the Merciful, the Compassionate
Peace, mercy and blessings of Allah upon you
Taken from al-jahafal and as-ansar

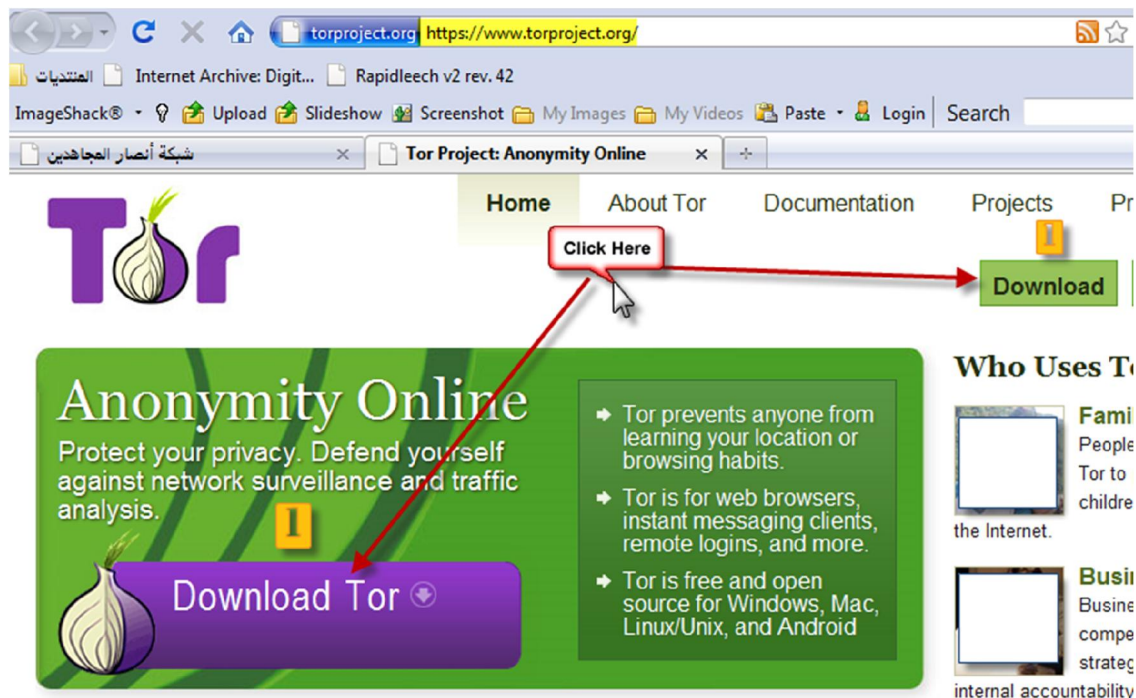
Brought to you by Abu Ink al Terra

Please spread this tutorial to increase awareness among my Beloved Brothers and Sisters on the Beloved Path!

1: Download and Install

Remember TOR only works with Firefox browser, when downloading try to get the bundle which includes firefox set to run TOR.

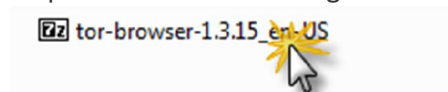
Step 1: Goto <https://www.torproject.org/> and click Download Tor



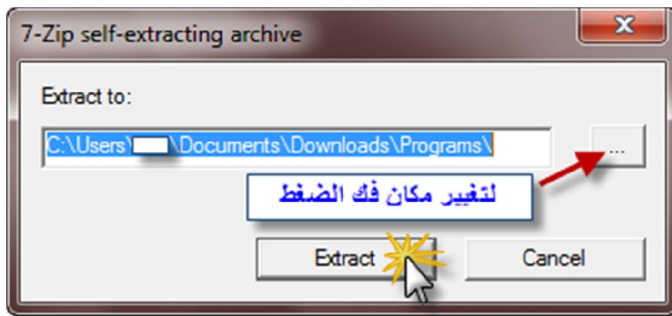
Step 2: select the latest bundle version includes a web browser fully configure for Tor. Select the one highlighted yellow as this is a portable version the green will leave traces



Step 3: once downloaded go to location of file double click to extract



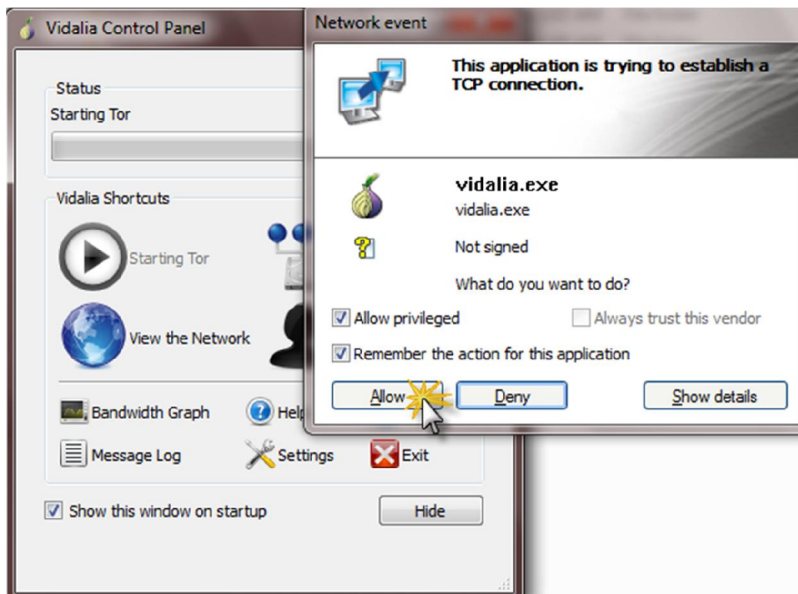
Step 4: Select location of where you wish to extract and select Extract



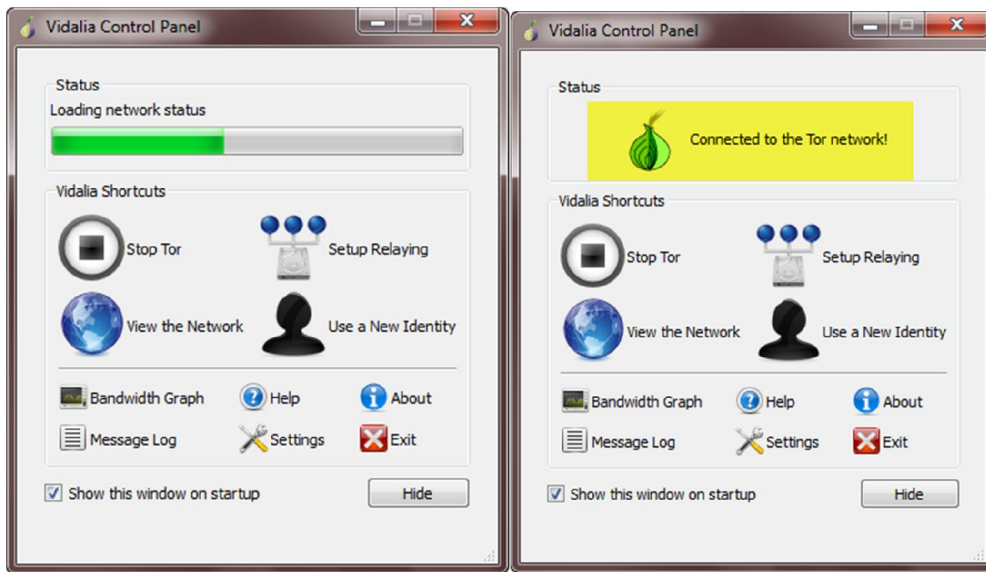
Step 5: Once extracted open location of extraction double click on Start Tor Program



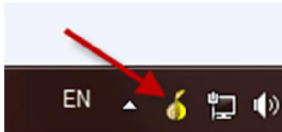
Step 6: click on Allow if your firewall or antivirus attempts to block the program



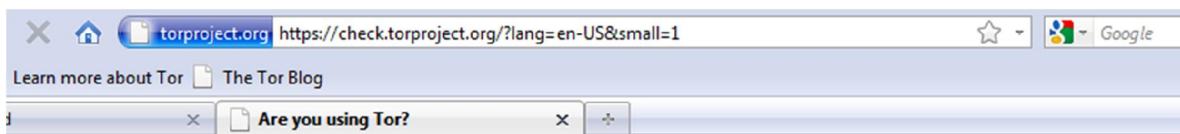
Step 7: Click on Start Tor



The shift to a green bulb means that Tor is working



If all goes well then a green onion should appear in the taskbar and web browser would popup saying the message below



Congratulations. Your browser is configured to use Tor.

Please refer to the [Tor website](https://www.torproject.org/) for further information about using Tor safely. You are now free to browse the Internet anonymously.

How To Test Tor and Check Our Identity

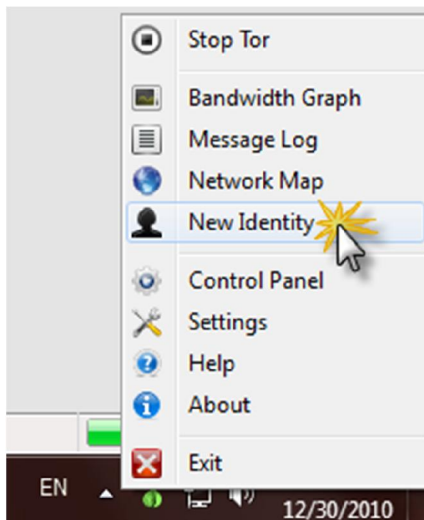
We now do a test to make sure that our identity has changed on the net,

Step 1: Go to <http://www.ip-adress.com> to check your ip/location

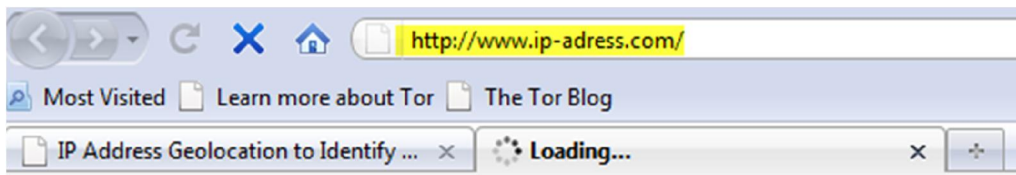
Note: a change in the country other than where you are.



If you wish to change your identity,
Right click on the onion and choose New Identity



Step 3: recheck the ip address



the result

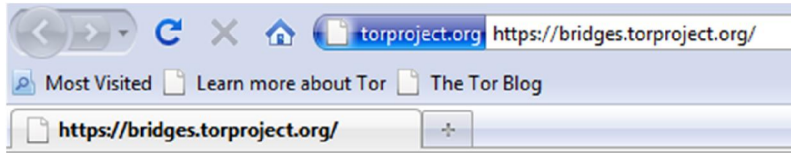
My IP address is: 192.168.1.1
My IP Address Location: in Sweden
ISP of my IP: ServerConnect Sweden AB

Bridges & How to obtain more

Bridges increases the speed of Tor, and will also increase the security of communication and prevent the prying eyes the dirty kuffar know that you are using Tor.

Step 1: go to <https://www.bridges.torproject.org/> or type in google tor Bridges

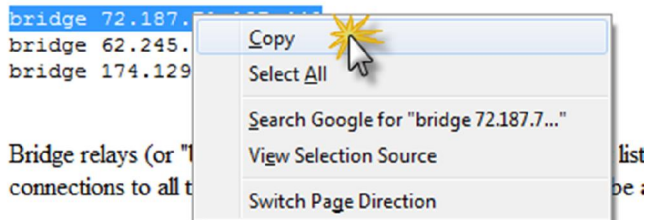
Type in the capthcha



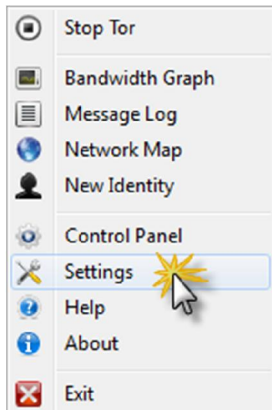
Here are your bridge relays:

```
bridge 72.187.71.187:443
bridge 62.245.118.9:443
bridge 174.129.218.239:9001
```

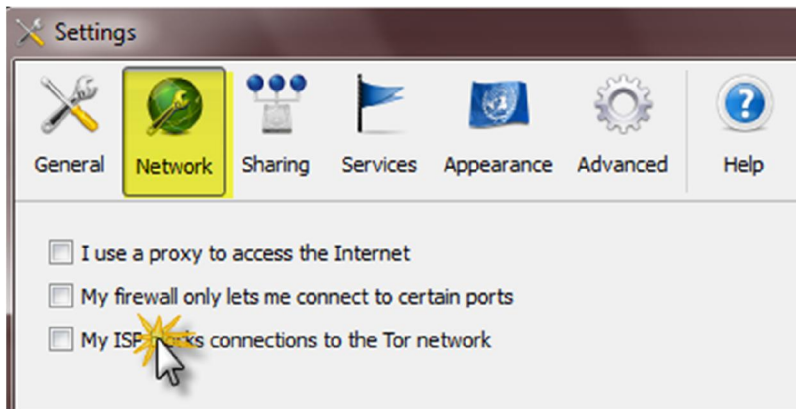
Step 2: highlight the first bridge right click and select copy



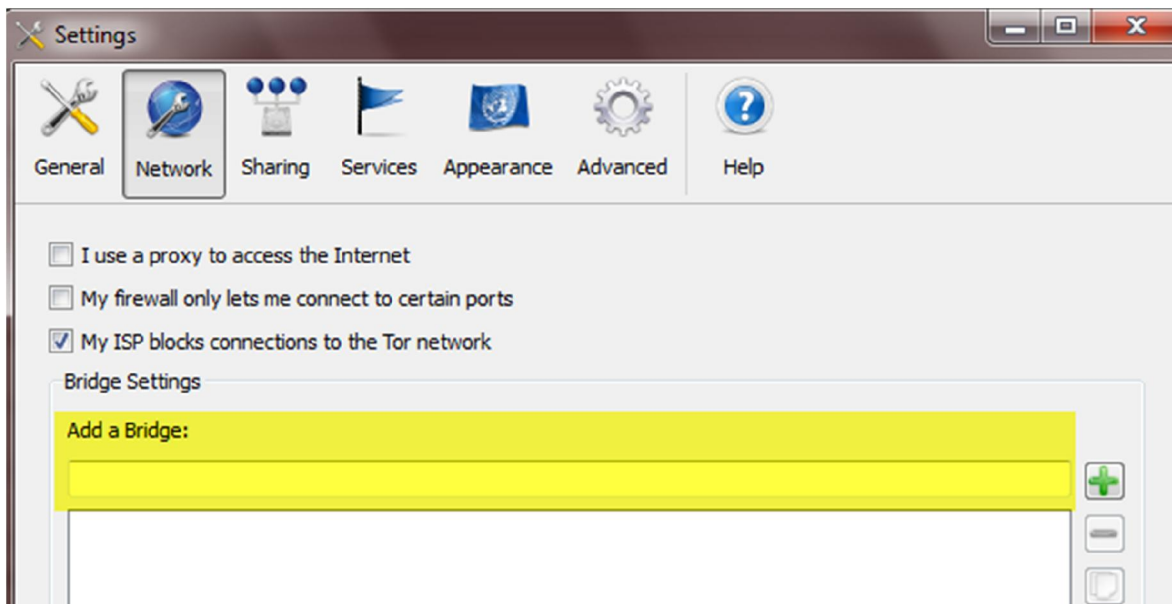
Step 3: Right click on the onion and click on settings



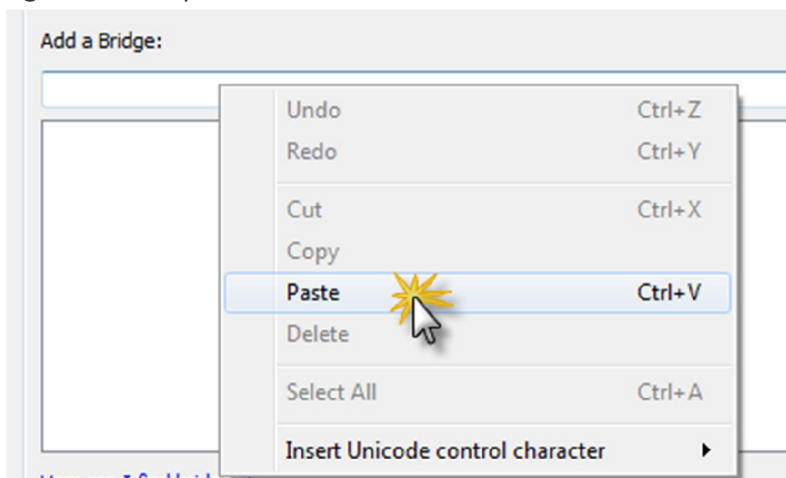
Step 4: in the main window of the Settings choose Network & Click on My ISP



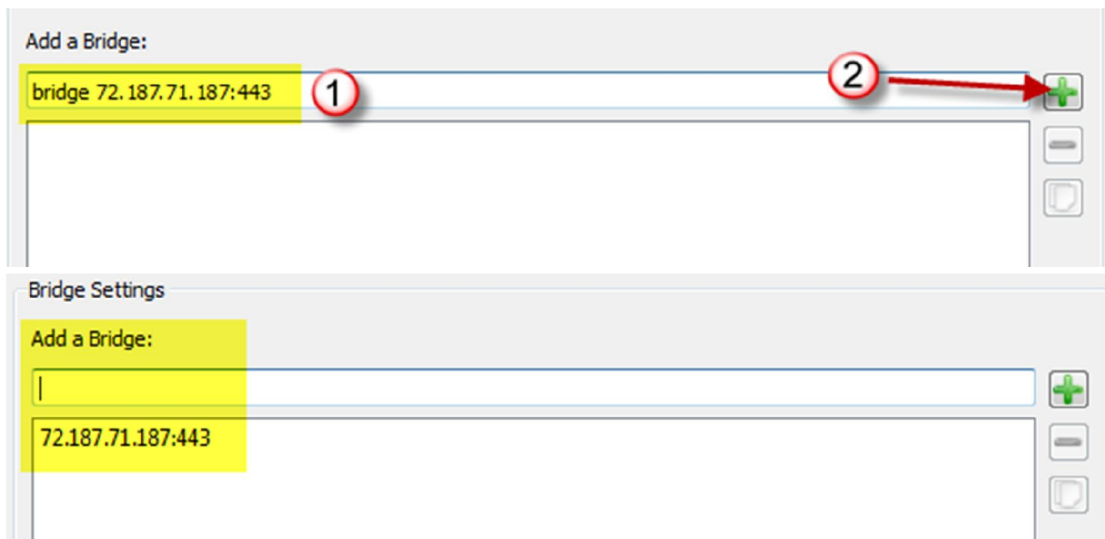
Step 5: a window will appears to add a bridge,



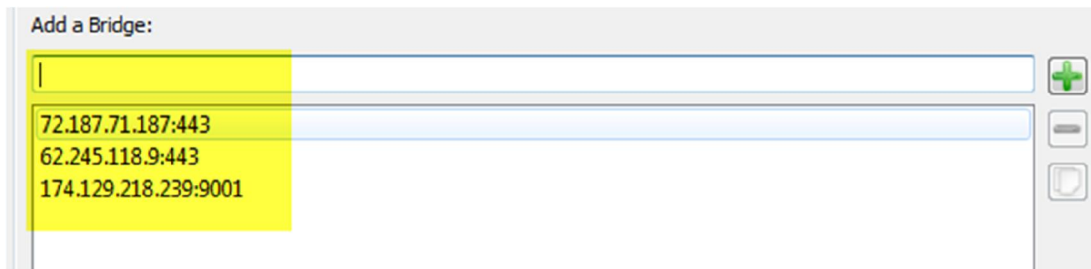
right click and paste



Step 6: to add the bridge click on the + sign

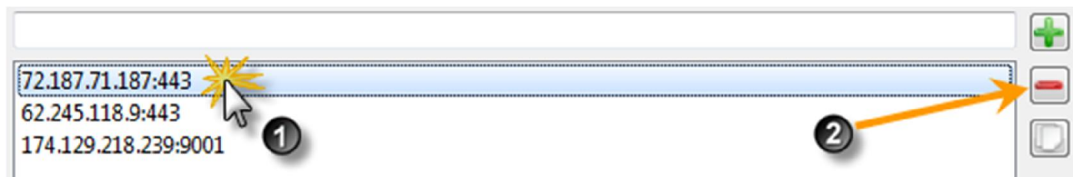


do likewise for all the bridges on the website



To delete a bridge

Select a bridge and click on the - sign

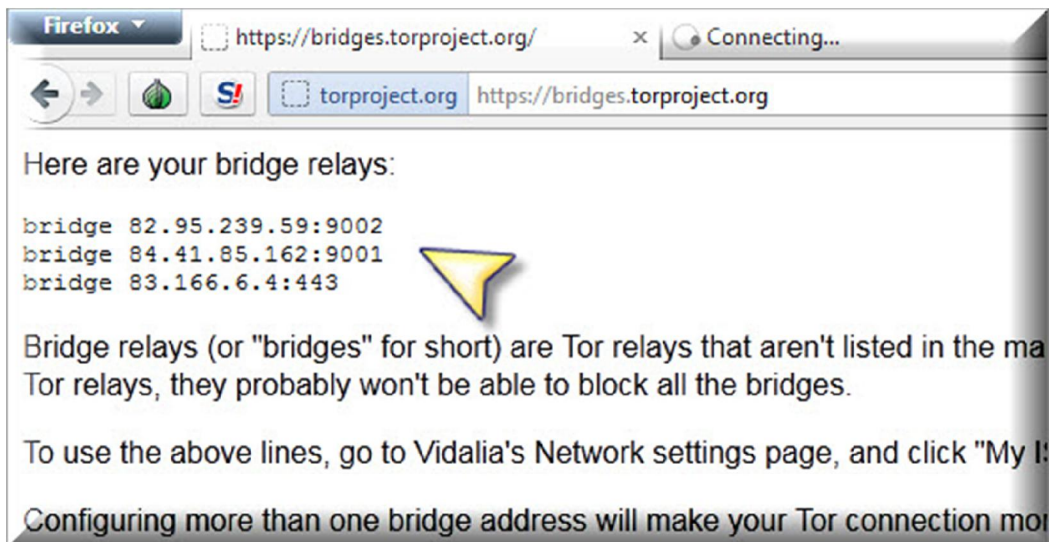


Once done click on OK

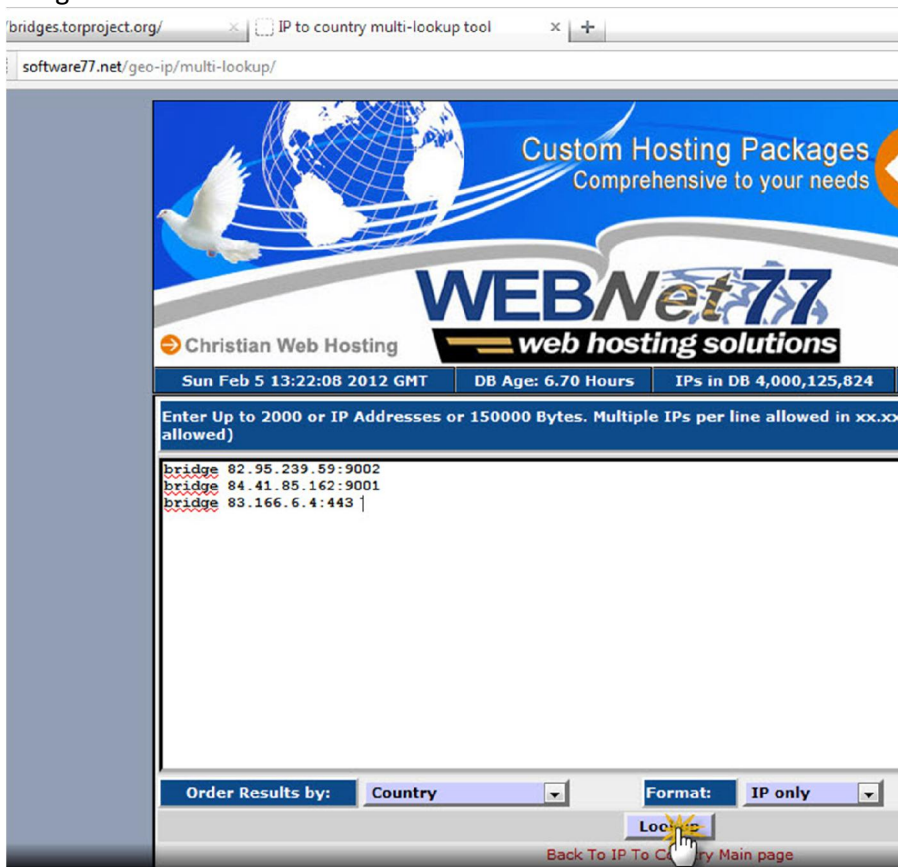
How to Filter Bridges

The purpose of this next tutorial is so that one can refrain from using the servers of the countries who are purely evil, Such as the so-called States of America and Israel

step 1: goto <https://bridges.torproject.org/>



open <http://software77.net/geo-ip/multi-lookup/> in a new page in your web browser and copy & paste the bridges as below



Click on Lookup

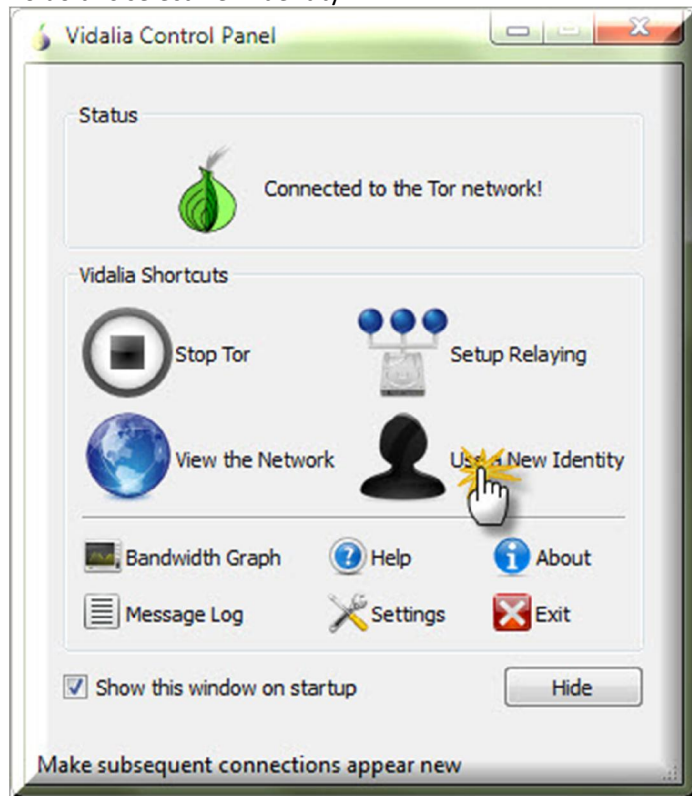
the three countries are listed below

```
# Created by: Webnet77.com
# Location : http://software77.net/geo-ip/multi-lookup/
# On : Sun Feb 5 13:22:53 2012
# Version : 5.8.1
# DB Age : 6.71 Hours
# Lines : 2
# Unique Ips: 3

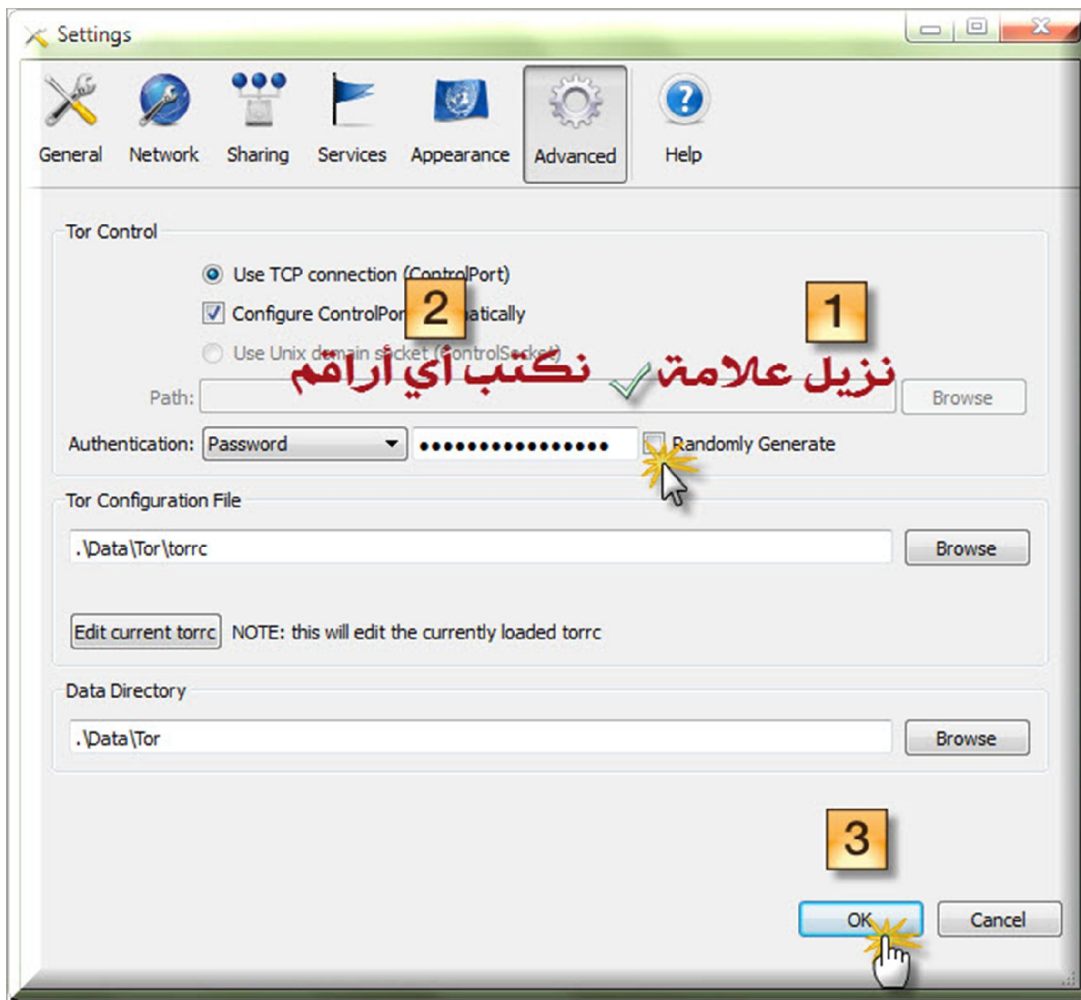
82.95.239.59 # NL Netherlands
83.166.6.4 # SE Sweden
84.41.85.162 # SI Slovenia
```

When choosing Bridges choose all countries except the countries of most evil of America, Israel and your home country

To do this select New identity

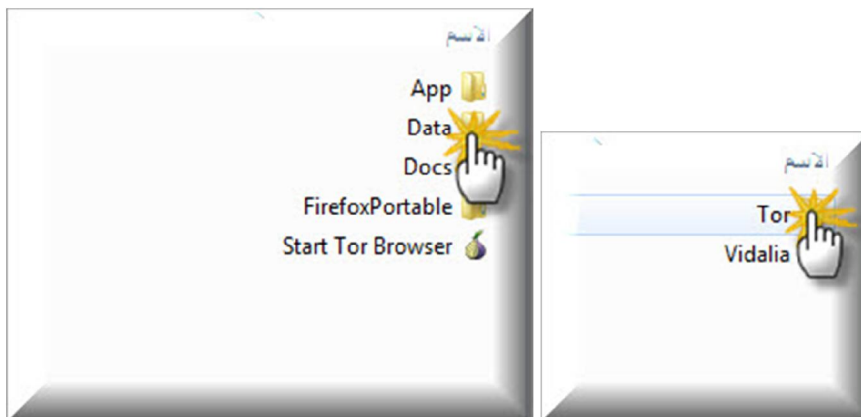


Choose settings (these steps only work at the beginning of the use of Taurus) & click on Advanced tab



Uncheck Randomly Generate and input a password

locate the torrc file Tor \Data\Tor





Double click on file "torrc" and open with notepad

```
# This file was generated by Tor
# The old torrc file was renamed
↓ كل ثلاثة أيام نستبدل البريدات
ApidDiskWrites 1
bridge هنا أقل عدد ثلاثة بريدات

ControlPort 9051
DataDirectory .\Data\Tor
DirReqStatistics 0
GeoIPFile .\Data\Tor\geoip
HashedControlPassword 16:2543705
Log notice stdout
SocksListenAddress 127.0.0.1
UseBridges 1
ExcludeNodes {IL},{DE}
ExcludeExitNodes {US},{GB}
StrictNodes 1
CircuitBuildTimeout 120
```

Delete this sentence

Code:

UpdateBridgesFromAuthority 1

And add this

Code:

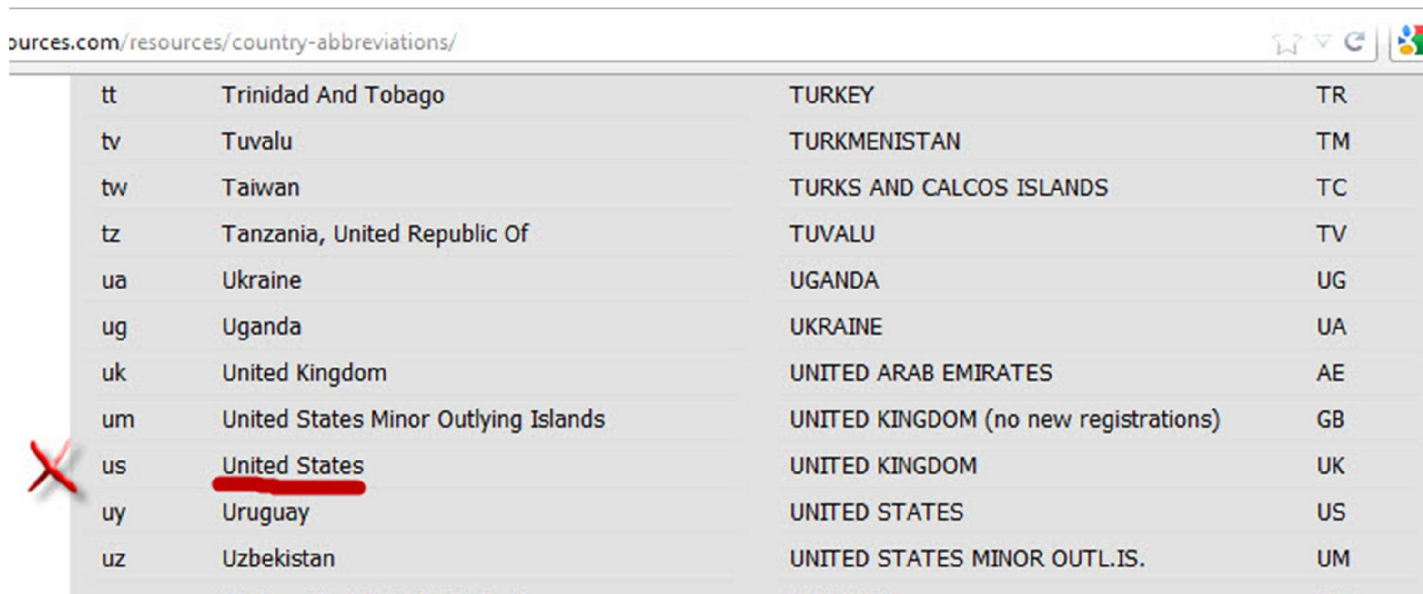
ExcludeNodes {IL},{DE}
ExcludeExitNodes {US},{GB}
StrictNodes 1
CircuitBuildTimeout 120

The first sentence to exclude the so-called Israel and Germany from all nodes in the Tor, so do not pass the Itisaluna

The second sentence

To exclude the so-called America and Britain in the last decade of Tor, which we reached our demand for a jihadist networks

Check the country code that you want to exclude at <http://www.greenbuilder.com/general/countries.html>



tt	Trinidad And Tobago	TURKEY	TR
tv	Tuvalu	TURKMENISTAN	TM
tw	Taiwan	TURKS AND CALCOS ISLANDS	TC
tz	Tanzania, United Republic Of	TUVALU	TV
ua	Ukraine	UGANDA	UG
ug	Uganda	UKRAINE	UA
uk	United Kingdom	UNITED ARAB EMIRATES	AE
um	United States Minor Outlying Islands	UNITED KINGDOM (no new registrations)	GB
 us	<u>United States</u>	UNITED KINGDOM	UK
uy	Uruguay	UNITED STATES	US
uz	Uzbekistan	UNITED STATES MINOR OUTL.IS.	UM

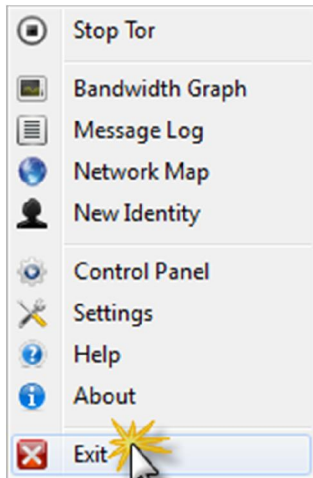
Remember to constantly change your bridges daily

If for some reason after following these procedures Tor refuses to work correctly, simply extract Tor again and start afresh

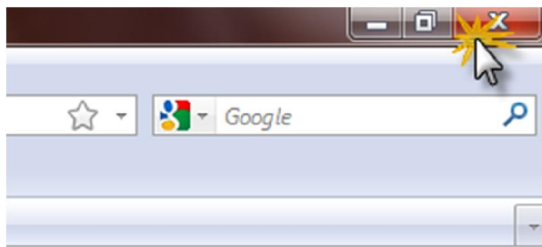
To Exit Tor



Simply right click on the onion in your taskbar and select exit



Or close the web browser



Notice the disappearance of the Tor onion



And the disappearance of the Web Browser.

Note: If you want to move the Tor Folder Taurus to another place or on a memory stick there is nothing wrong with that and its settings will remain unchanged Insha Allah!

Praise be to Allah, Lord of the Worlds